Online Child Predator Prevention & Citizen Reporting Act (CRA Act) (1st Draft)

Legislative Proposal

By: Jungheon Kwak | jhbryan0817@gmail.com | The University of Hong Kong

1st September 2025

Abstract

Current law-enforcement sting operations are resource-intensive and limited in scope, with only a small number of cases pursued each year despite the vast scale of online predatory solicitation. By contrast, the online environment is already saturated with uncertified, unlawful "catfishing" and extortion attempts, which predators routinely encounter far more often than legitimate stings. Although these actors operate outside the law, their sheer scale has created a powerful deterrent effect: predators approach online interactions with heightened fear and paranoia, altering their behavior precisely because they cannot easily distinguish a scammer from a real investigation. This behavioral impact—driven by the perception of constant risk—is far larger than that achieved by formal sting operations alone. The CRA Act provides a systemic way to harness this same scale of deterrence in a lawful, accountable, and evidence-preserving framework, while introducing offender-funded financial incentive mechanisms to sustain broad participation without public expense. By shifting this dynamic from the shadows into a regulated channel, the Act converts an already-demonstrated deterrent force into a reliable, controlled, constitutional, and self-funding system for child protection.

Section 1. Short Title; Purpose; Findings

(a) Short Title. This Act may be cited as the "Online Child Predator Prevention & Citizen Reporting Act" or the "CRA Act."

(b) Purpose. To protect children from online sexual exploitation by certifying civilian volunteers to detect, document, and report suspected online predatory conduct under strict safeguards, while leaving all investigative and prosecutorial decisions to law enforcement.

(c) Legislative Findings.

1. A substantial share of initial grooming and exploitation begins online.

2. Law enforcement resources are finite; standardized civilian reporting can serve as a force multiplier when tightly regulated.

3. Predatory solicitation of a known or perceived minor is illegal speech integral to criminal conduct and not protected by constitutional free-speech guarantees.

4. This Act is designed to preserve due process, evidentiary integrity, privacy, and safety, and to operate without net public cost through an offender-funded mechanism.

Section 2. Definitions

1. Online Safety Reporter (OSR): A private civilian above the age of 18 who completes the certification described in Section 3 and acts in compliance with this Act and its rules. OSRs are not law enforcement officers or agents of the state.

2. Minor Representation: An online persona operated by an OSR that clearly and truthfully declares an age under eighteen (minimum representable age: 16).

3. Explicit Communication: Written, visual, or audio content of a sexual nature directed toward a persona identified as a minor.

4. Predatory Conduct: Any attempt by an adult to initiate, encourage, or escalate explicit communication after being informed the other party is under eighteen, or any attempt to entice, solicit, or exploit a person believed to be under eighteen.

5. Portal: The secure digital submission system designated by the responsible agency for receiving OSR reports and materials.

6. Board: The Online Safety Oversight Board established under Section 10.

Section 3. Certification; Code of Conduct

(a) Certification. The responsible agency shall provide a comprehensive online curriculum and assessment covering: child-protection law, enticement/solicitation elements, evidence preservation, privacy, and OSR prohibitions.

(b) Code of Conduct (required for certification and rewards). An OSR shall:

1. Declare age early: Clearly state “I am 16/17” at or near the outset of any pertinent conversation and preserve that message.

2. Never initiate sexual content: The suspect must take the first illegal step; OSR responses must remain non-provocative and non-leading.

3. No images of real minors: OSR personas may not use photographs or media of actual minors; only neutral avatars or adult stock images are permitted.

4. No physical meetings: Arranging or attending in-person meetings is prohibited.

5. No publicity: Public exposure or media posting of suspects/evidence is prohibited.

6. Full preservation: Retain complete, unedited logs and relevant metadata; no selective screenshots.

7. Affidavit: Submit a sworn statement under penalty of perjury that the submission is complete and accurate.

(c) Decertification. The agency may suspend or revoke certification for violations, with notice and an administrative appeal process.

Section 4. Authorized and Prohibited Activities

(a) Authorized. An OSR may:

1. Operate a Minor Representation (16–17) and initiate non-explicit conversation
2. Preserve and submit communications after an adult continues post-age-declaration.

(b) Prohibited. An OSR shall not:

3. Initiate sexual discussion, steer or pressure toward sexual content, or fabricate messages.
4. Arrange/attend in-person meetings.
5. Conduct doxxing, harassment, or public dissemination of materials.
6. Direct or coordinate arrests, confrontations, or surveillance.
7. Use spyware, hacking, unlawful recording, or any illegal means of data collection.

Section 5. Reporting; Chain of Custody; Law Enforcement Control

(a) Portal Submission. OSRs shall submit: (i) raw chat exports where supported by the platform, (ii) full message histories, (iii) timestamps, usernames/IDs, URLs, and device/application info, and (iv) the OSR affidavit.
(b) Chain of Custody. The agency shall issue receipt IDs; preserve submissions; and maintain verifiable chain-of-custody records.
(c) Lawful Verification. Law enforcement may seek platform and subscriber records through appropriate legal process (warrants/subpoenas).
(d) Exclusive Authority. Only law enforcement may make investigative, charging, or prosecutorial decisions or initiate contact with suspects.

Section 6. Evidentiary Safeguards and Constitutional Construction

(a) Private Actor Status. OSRs act as private reporters, not as agents of the state. This Act does not create any prior agreement, encouragement, or knowledge by the government that would transform OSR activities into state action.
(b) Non-Entrapment Design. The “no sexual initiation” rule under Section (4)b exists to ensure the suspect voluntarily undertakes illegal conduct.
(c) First Amendment Compliance. This Act targets conduct—enticement/solicitation of a perceived minor—not protected expression.
(d) Due Process. Nothing in this Act alters the state’s burden of proof, available defenses, or discovery obligations. OSR submissions shall be subject to full evidentiary review, with defendants entitled to challenge authenticity, completeness, or bias under existing rules of evidence.

(e) Equal Protection. Enforcement shall be neutral as to race, religion, sex, national origin, and other protected characteristics.
(f) This Act shall be construed narrowly to preserve constitutional rights and avoid any interpretation that could render it invalid. If any provision conflicts with federal or state constitutional requirements, it shall be reformed to the minimum extent necessary to comply, prioritizing child safety within lawful bounds.

Section 7. Liability; Immunities; Penalties for Abuse

(a) Safe Harbor. An OSR who substantially complies with this Act and rules is not civilly or criminally liable for minor impersonation or good-faith evidence preservation.
(b) Loss of Protection. Safe harbor is forfeited if the OSR does not comply with due process as outlined in Section (3)b and Section (4)
(c) Penalties. Violations may result in decertification, reward forfeiture, civil liability, and prosecution under existing law.

Section 8. Rewards; Eligibility; Process

(a) Eligibility. Rewards may be granted only when:
1. The OSR was certified before the interaction;
2. The OSR complied with Section 3(b) and Section 4; and
3. The case results in charges filed or conviction for predatory conduct or an equal/greater offense.
(b) Factors. Reward amounts shall consider: offense severity; evidentiary quality; resource savings; and fund solvency.
(c) Timing; Transparency. Rewards are payable after final disposition (including appeals windows as set by rule). The Board shall publish aggregate reward statistics annually.
(d) No General Fund Obligation. Rewards are contingent on the availability of the Fund described in Section 9; if insolvent, payments are queued until replenishment.

Section 9. Self-Funding Mechanism

(a) Child Online Safety Fund ("Fund"). Create a dedicated, segregated Fund administered by the Board.
(b) Sources. The Fund shall consist solely of:
1. Fines, penalties, court costs, and lawful assessments imposed upon defendants convicted in cases initiated through OSR reports;

2. Lawfully seized and forfeited assets attributable to such convictions;

3. Voluntary donations or grants.
(c) Uses. The Fund may be used only for: OSR training and certification; portal maintenance; oversight and audits; and rewards under Section 8.
(d) Safeguards. Courts retain discretion to avoid unconstitutional excessive fines and to consider indigency. The state bears no obligation to backfill the Fund.
(e) Non-Supplant. Fund revenues shall not supplant existing victim-assistance or

child-protection appropriations.

Section 10. Online Safety Oversight Board; Audits; Rulemaking

(a) Board. Establish an independent Board comprising: child-protection and digital-forensics experts; a prosecutor; a defense/constitutional law expert; a victim-advocate; a technologist; and a member of the public.

(b) Duties.

1. Adopt rules for certification, code of conduct, reporting, data retention, rewards, and conflicts of interest;
2. Administer the Fund;
3. Publish an annual public report (submissions, referrals, charges, convictions, reward totals, training throughput);
4. Commission independent audits at least every three (3) years.

(c) Data Minimization. Retention schedules shall minimize storage of personally identifiable information consistent with evidentiary needs.

(d) Rulemaking. The responsible agency shall promulgate rules consistent with this Act within nine (9) months of enactment.

Section 11. Privacy; Data Security; Victim Protection

(a) Redactions. Prior to public reporting, victim and witness identifiers shall be removed.

(b) Security. The portal and evidence repositories shall meet or exceed applicable cybersecurity standards (e.g., FedRAMP/ISO-27001 equivalents).

(c) Prohibition on Secondary Use. OSR-submitted data shall not be used for marketing, profiling, or non-law-enforcement purposes.

Section 12. Pilot; Evaluation

(a) Pilot. Initial two-year pilot with capped certifications and periodic evaluations.

(b) Metrics. Time-to-charge, conviction rates, dismissal/declination reasons, fund solvency, and civil-liberties complaints.

(c) Legislative Review. Continued operation contingent on a public performance report and legislative reauthorization.

Section 13. Severability

If any provision is held invalid or unconstitutional, remaining provisions shall remain in force.